PN - JP2000216822 A 20000804
PD - 2000-08-04
PR - JP19990016634 19990126
OPD - 1999-01-26
TI - METHOD FOR ALLOCATING IP ADDRESS
IN - ONUMA TETSUYA
PA - HITACHI LTD
IC - H04L12/56 ; G06F13/00 ; G06F15/00 ; H04L12/28
© WPI / DERWENT

TI - Internet protocol address assigning procedure for computer network system, identifies input physical characteristic based on input authentication data upon reception of data through communication unit
PR - JP19990016634 19990126
PN - JP2000216822 A 20000804 DW200108 H04L12/56 007pp
PA - (HITA) HITACHI LTD
IC - G06F13/00 ;G06F15/00 ;H04L12/28 ;H04L12/56
AB - JP2000216822 NOVELTY - The input physical characteristic of a user is identified based on an input authentication data upon reception of data through a communication unit. The communication unit is interconnected to many data processors.
- USE - For computer network system.
- ADVANTAGE - Maintains security when assigning internet protocol address. Ensures reliable assignment of internet protocol address.
- DESCRIPTION OF DRAWING(S) - The figure shows the flowchart of an internet protocol address assigning procedure.
- (Dwg.2/4)
OPD - 1999-01-26
AN - 2001-064719 [08]
© PAJ / JPO

PN - JP2000216822 A 20000804
PD - 2000-08-04
AP - JP19990016634 19990126
IN - ONUMA TETSUYA
PA - HITACHI LTD
TI - METHOD FOR ALLOCATING IP ADDRESS
AB - PROBLEM TO BE SOLVED: To provide a method for allocating an IP address, which can maintain security, by inputting the physical feature of a user and transmitting/receiving inputted certification data as a user identifier through a communication means.
- SOLUTION: When the allocation request of an IP address for accessing a specified segment and a server is generated in an arbitrary terminal machine 20-1, the terminal machine 20-1 inputs a physical feature, a fingerprint, for example, by using a fingerprint certification device 30-1. The fingerprint data is transmitted to a certification server 10 through a public network 70. The certification server 10 executes the collation processing of whether registered data stored in the certification server 10 and the user identifier of fingerprint data are the same or not in accordance with the reception of fingerprint data. When the results of the collation processing are matched, the specified IP address is allocated to a user and the

collation result is transmitted to the terminal machine 20-1. When the results of the collation processing are not matched, the allocation of the IP address is judged to be impossible and the effect is transmitted.

I - H04L12/56 ;G06F13/00 ;G06F15/00 ;H04L12/28

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－216822
（P2000－216822A）
(43)公開日　平成12年８月４日(2000.8.4)

(51)Int.Cl.'		識別記号	FI		テーマコード'（参考）
H04L	12/56		H04L	11/20	102D　5B085
G06F	13/00	351	G06F	13/00	351Z　5B089
	15/00	330		15/00	330F　5K030
H04L	12/28		H04L	11/00	310Z　5K033

審査請求　未請求　請求項の数３　ＯＬ　（全７頁）

(21)出願番号　特願平11－16634

(22)出願日　平成11年１月26日(1999.1.26)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　大沼　哲也
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所情報システム事業部内
(74)代理人　100068504
弁理士　小川　勝男

最終頁に続く

(54)【発明の名称】　ＩＰアドレスの割当て方法

(57)【要約】
【課題】外部からリモート・アクセスで使用する場合に、指紋認証を用いることによって「なりすまし」等を防止した特定ＩＰアドレスの割当てができるようにする。
【解決手段】割当て後、ある一定時間端末機２０－１が利用されていない場合、端末機２０－１に格納された指紋データと指紋認証装置３０－１より入力した照会指紋データを照合し、この照合結果に応じた利用の継続を決定することによって機密保持を維持する。

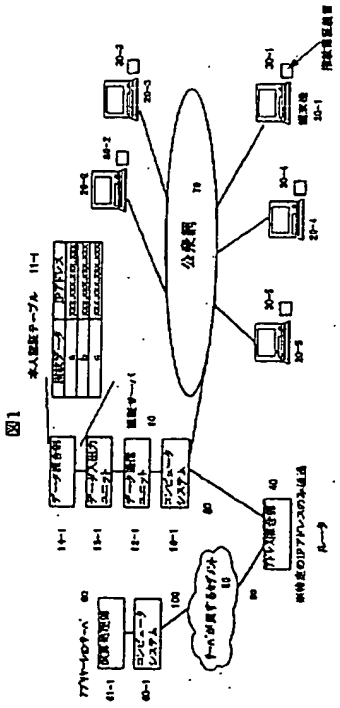


図1

【特許請求の範囲】
【請求項１】複数のデータ処理手段と複数のデータ処理手段を相互接続する通信手段において、利用者の身体的特徴を入力し、入力した認証データを利用者識別子として通信手段を介して送受するコンピュータネットワークシステムを有することを特徴とするＩＰアドレスの割当て方法。
【請求項２】複数のデータ処理手段と複数のデータ処理手段を相互接続する通信手段とを有するコンピュータネットワークシステムにおける特定のＩＰアドレスの割当て方法であって、利用者の身体的特徴を入力し、入力した認証データを利用者識別子として前記通信手段を介して送受する利用者識別子と照合し、照合結果にしたがって、特定のＩＰアドレス割当てを決定する方法を有することを特徴とするＩＰアドレスの割当て方法。
【請求項３】前記特定のＩＰアドレス割当てを決定する方法は、ある一定時間端末機が利用されていない場合において、利用者の身体的特徴を再問合せし、再入力した認証データを利用者識別子として照合し、照合結果にしたがって、特定のＩＰアドレス利用の継続を決定する方法を有することを特徴とするＩＰアドレスの割当て方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、イントラネット上の特定サーバや特定セグメントを外部から利用するために特定ＩＰアドレスを割当てる方法に関し、特に、身体的特徴による本人認証によって本人のみ利用可能にするためのＩＰアドレスの割当て方法である。
【０００２】
【従来の技術】複数のコンピュータシステムを通信網により相互に接続したコンピュータネットワークシステムでは機密保護のため、ネットワークシステムへのアクセス要求に応じて利用者を識別し、それを達成するために特定のＩＰアドレスを割当て特定のセグメントやサーバにアクセスする処理を行なう必要がある。
【０００３】現状、特定のＩＰアドレスを割当てする方法としては、Ｍａｃアドレスによって特定の端末に割当てする方法やパスワード入力によって特定の利用者に割当てすることができる。
【０００４】
【発明が解決しようとする課題】上述したようなコンピュータネットワークシステムにＭａｃアドレスやパスワード入力による認証を用いてコンピュータシステムまたはネットワークシステムにアクセスを行なう従来の方法では、厳密な機密保護が困難であるという問題点がある。
【０００５】従来の特定ＩＰアドレスの割当て方法では、特定の端末機やパスワードを知っている者の利用に対する機密保護については有効である。しかし、本人以外に利用が認められないケースにおける機密保護については、例えば、パスワードは本当に本人しか知らないのか、あるいは、いわゆる「なりすまし」によって他人が不正に利用していないのか等を確認することが困難である。
【０００６】上述の課題から、本発明の目的は、機密保護を維持することが可能なＩＰアドレスの割当て方法を提供することである。
【０００７】
【課題を解決するための手段】この発明に係るコンピュータネットワークシステムにおいて、複数のデータ処理手段は、ＩＰアドレスの割当て要求に対して利用者識別子を送出し、通信手段に接続され、前記通信手段を介して受け取った利用者識別子を、予め登録された利用者識別子と照合し、ＩＰアドレス割当ての可否を判定する照合手段を具備することを特徴とする。
【０００８】この発明に係るＩＰアドレス割当て方法は、複数のデータ処理手段と複数のデータ処理手段を相互接続する通信手段とを有するネットワークシステムにおけるＩＰアドレス割当て方法であって、割当て要求に応じ、利用者の身体的特徴を入力し、前記認証データを利用者識別子として前記通信手段を介して受信し、照合の結果得られる利用者の特定のＩＰアドレスを送信することを具備している。
【０００９】前記ＩＰアドレス割当て方法は更に、前記通信手段を介して受信される利用者識別子を、予め認証サーバに登録された利用者識別子と照合し、照合結果に従って、特定ＩＰアドレスの割当てを決定することを具備している。
【００１０】以上のＩＰアドレス割当て方法においては、人間の身体的特徴を有する認証データ、本件においては指紋に依存するものであり、各個人に固有のものである。従って、この認証データを利用者識別子として用いてネットワークシステムに対する特定のＩＰアドレスの割当てを決定すれば、認証データが登録されていない他人による特定セグメントや特定サーバへのアクセスに対して、Ｍａｃアドレスやパスワード入力による割当てよりも確実な機密保護ができる。
【００１１】
【発明の実施の形態】以下、この発明を図面を参照して説明する。図１は、この発明のシステムの概略構成を示すブロック図である。同図に示されるように、複数のコンピュータシステムである認証サーバ１０や端末機２０－１～２０－５が公衆網７０を介して相互に接続されている。端末機２０－１～２０－５には利用者の身体的特徴（認証データ）を入力する指紋認証装置３０－１～３０－５が各々接続されている。
【００１２】前記公衆網７０には、端末機２０－１より送信された認証データに基づいてコンピュータネットワークシステムに対する利用者が特定セグメントやサーバ

にアクセスすることが可能な特定のＩＰアドレスを決定する認証サーバ１０が接続されている。この認証サーバ１０は端末機２０－１から公衆網７０を介して送られる認証データとこのコンピュータネットワークにおいて予め本人認証テーブル１１－１（図３）として登録されている指の特徴データとを照合し、この特徴データと一致した場合、本人認証テーブル１１－１に登録されている特定のＩＰアドレスを割当てる。端末機２０－１は、このＩＰアドレスによって、特定のセグメント５０およびアプリケーションサーバ６０にアクセスする。

【００１３】次に、このコンピュータネットワークシステムにおける端末機２０－１および認証サーバ１０のＩＰアドレスの割当て処理を図２のフローチャートに示す。

【００１４】コンピュータネットワークシステムにおいて、任意の端末機２０－１で特定のセグメントおよびサーバをアクセスするためのＩＰアドレスの割当て要求が発生すると、この端末機２０－１では指紋認証装置３０－１を用いて身体的特徴、本件においては指の指紋を入力する（２０１）。この指紋データを、公衆網７０を介して認証サーバ１０に送出される（２０２）。

【００１５】認証サーバ１０では、指紋データの受信に応じ、認証サーバ１０に格納されている登録データと、前記指紋データの利用者識別子が同一であるか照合処理が行なわれる（２０３，２０４）。照合処理の結果が一致である場合、利用者に対し、特定のＩＰアドレスが割当てられ、照合結果を端末機２０－１に送信される（２０５，２０６）。一致しない場合は、ＩＰアドレス割当て不可と判断され、この旨が送信される（２０７，２０８）。

【００１６】その後、端末機２０－１では割当て結果を端末利用者に表示する（２０９）。さらに、ＩＰアドレスが通知されたかを確認し、アドレスが割当てられた場合には端末機２０－１に登録され、指紋データも格納される（２１０，２１１）。

【００１７】次に、端末機２０－１に特定ＩＰアドレスを割当てた後の継続利用処理を図４のフローチャートに示す。ある一定時間端末機２０－１が利用されていない場合、端末機２０－１は利用者に対し、身体的特徴の照合を要求する（４０１）。利用者は再度、指紋認証装置３０－１を用いて身体的特徴を入力する（４０２）。指紋認証装置３０－１より照合指紋データを転送された端末機２０－１は、ＩＰアドレス割当て時に格納した指紋データと照合する（４０３，４０４）。データが一致した場合には、端末機２０－１のネットワークシステム上での利用が継続して利用できる（４０５）。データが一致しない場合には、照合指紋データを認証サーバ１０に送信する（４０６）。

【００１８】認証サーバ１０では、照合指紋データと登録データを照合する（４０７，４０８）。データが一致しない場合には、端末機２０－１に登録されていたＩＰアドレスを消去し、ネットワークシステムのコネクションが切断される（４０９，４１０）。データが一致した場合には、認証サーバ１０の登録データを端末機２０－１に送信される（４１１）。

【００１９】端末機２０－１では、登録データが通知された場合、指紋データを更新する（４１２，４１３）。

【００２０】以上説明したように、この方法によれば人間の身体的特徴を示すデータを利用者識別子となる認証データとして、予め登録されている登録データと比較照合することでネットワークシステムにおける特定のＩＰアドレスの割当ての可否が決定される。さらに、利用者の利用が中断した場合に、身体的特徴を示すデータを用いた再照会におけるＩＰアドレスの継続利用の可否が決定される。

【００２１】これにより、登録データに登録されていない他人によるアクセスに対してＭａｃアドレスやパスワード入力による特定ＩＰアドレスの割当てよりも確実な機密保護を実現できる。

【００２２】

【発明の効果】以上詳述したように、この発明によれば、コンピュータシステムにおいて身体的特徴データを用いたＩＰアドレスの割当てにより、例えばイントラネットを利用する外部利用者からの利用要求に対するＩＰアドレス割当てが、確実に機密保護を維持することが可能となる。

【００２３】特に、人間の身体的特徴を示す特徴を抽出して得られる認証データを利用者識別子として、予め登録されている登録データと比較照合することでネットワークシステムに接続する端末機に対する特定のＩＰアドレス割当ての可否が決定される。これにより、登録データが登録されていない他人によるイントラネットのアクセスに対して、Ｍａｃアドレスやパスワード入力によるＩＰアドレスの割当てを用いてアクセスするよりも確実な機密保護を実現できる。

【図面の簡単な説明】

【図１】本発明の実施例におけるシステム構成を示すブロック図。

【図２】本発明の実施例におけるＩＰアドレス割当て処理を示すフローチャート。

【図３】本発明の実施例における本人認証テーブルを示す図。

【図４】本発明の実施例における継続利用処理を示すフローチャート。

【符号の説明】

１０…認証サーバ、２０－１～４…端末機、３０－１～４…指紋認識装置、４０…ルータ、５０…サーバが属するセグメント、６０…アプリケーションサーバ、７０…公衆網、８０，９０，１００…通信回線、１１－１…本人認証テーブル。

【図1】

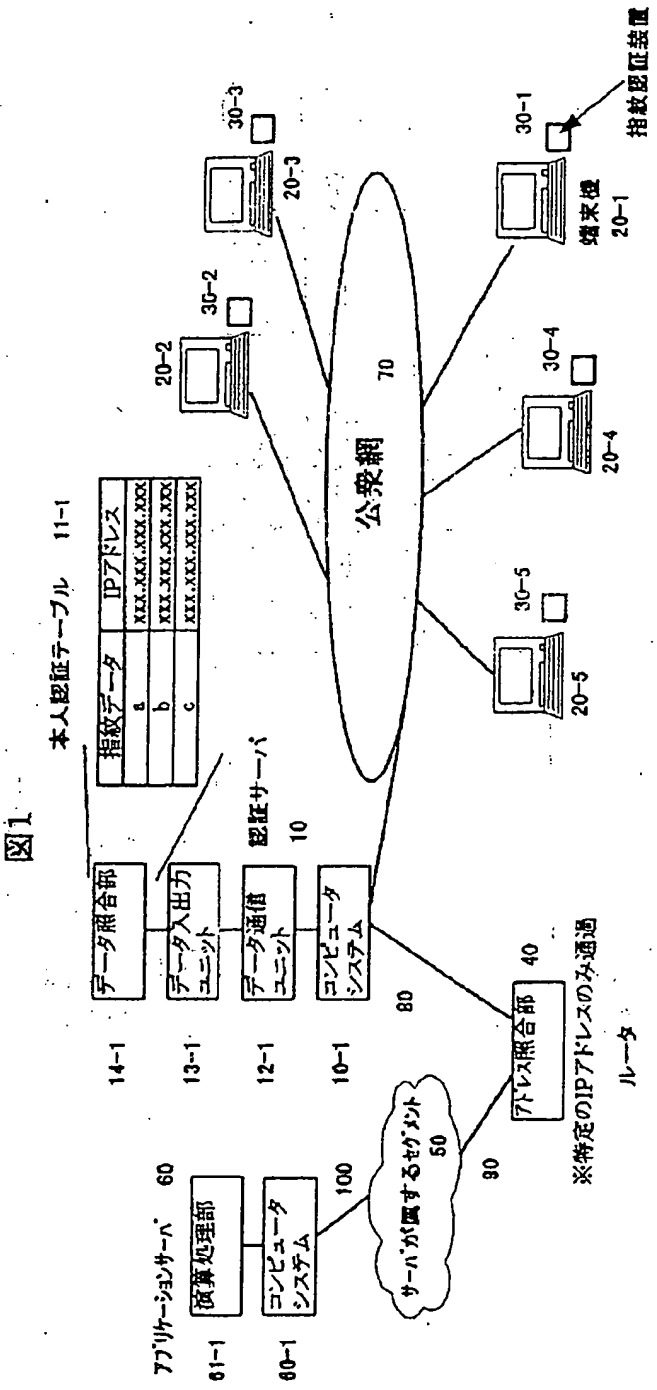


図1
本人認証テーブル 11-1
指紋データ
IPアドレス
a
b
c
xxx.xxx.xxx.xxx
xxx.xxx.xxx.xxx
xxx.xxx.xxx.xxx
認証サーバ 10
データ照合部 14-1
データ入出力ユニット 13-1
データ通信ユニット 12-1
コンピュータシステム 10-1
80
公衆網 70
20-2
30-2
20-3
30-3
30-1
指紋照合装置
端末機 20-1
30-4
20-4
30-5
20-5
アドレス照合部 40
ルータ
※特定のIPアドレスのみ通過
90
サーバが置するセグメント 50
100
コンピュータシステム 60-1
演算処理部 61-1
アプリケーションサーバ 60

【図2】

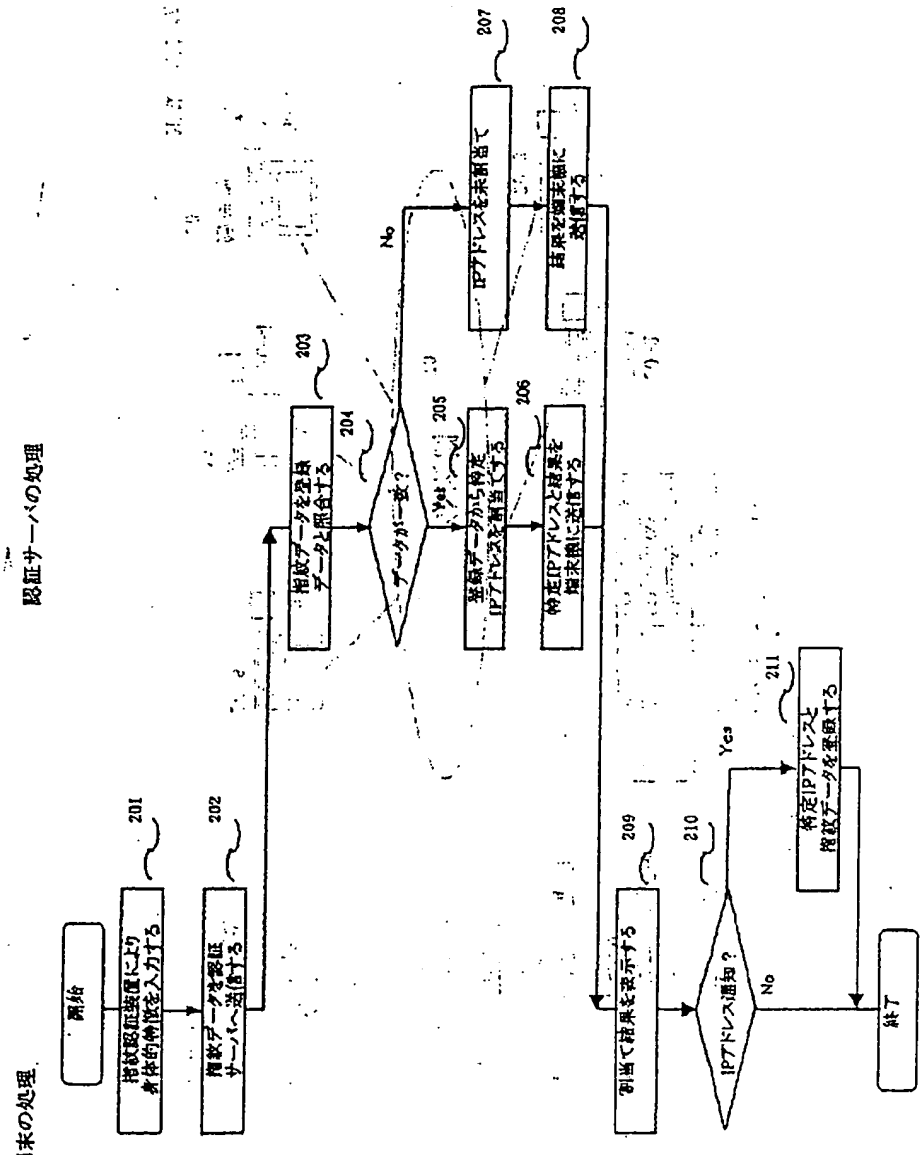

端末の処理
認証サーバの処理
開始
201
指紋認証装置により身体的特徴を入力する
202
指紋データを認証サーバへ送信する
203
指紋データを登録データと照合する
204
データが一致?
No
Yes
205
登録データから特定IPアドレスを割当てる
206
特定IPアドレスと結果を端末側に送信する
207
IPアドレスを未割当て
208
結果を端末側に送信する
209
割当て結果を表示する
210
IPアドレス通知?
No
Yes
211
特定IPアドレスと指紋データを登録する
終了

図2

【図3】

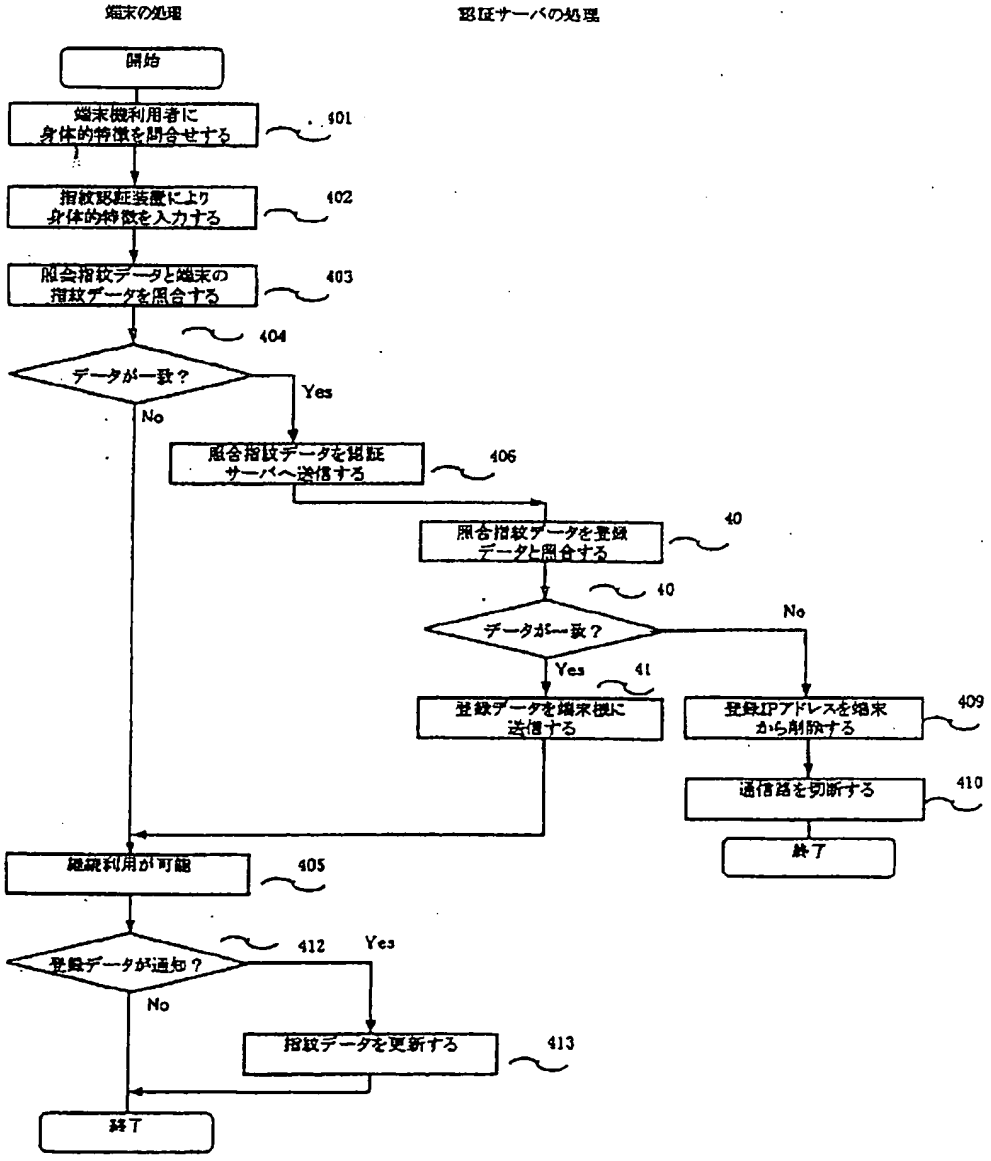
図3

指紋データ	IPアドレス
a	xxx.xxx.xxx.xxx
b	xxx.xxx.xxx.xxx
c	xxx.xxx.xxx.xxx

※テーブル中のIPアドレスは各1で全てユニーク

【図4】

図4



フロントページの続き

Fターム(参考) 5B085 AE23 AE26 BG07
5B089 GA21 GB01 HA10 JB22 KA17
KB06 KB13 KC29 KC47 KC58
LB10
5K030 GA15 HA08 HC01 HC14 HD06
HD09 LD18 LD20
5K033 AA08 BA04 CB08 DA06 EC03